Guidelines on Computer Maintenance for Computers with Controlled Unclassified Information (CUI)

Projects identified as containing Controlled Unclassified Information (CUI), have strict guidelines specified in the contract that control access to the information and auditing of access. Computer systems that store or process CUI data have a Technology Control Plan (TCP) mapping that ensures the computer is secured physically as well as electronically, based on the controls written into the contract.

ETS staff must follow several guidelines when performing maintenance on TCP computer systems.

1. Export Control orientation class:
   ETS staff must take the 1-hour Export Control orientation class prior to performing any work on a TCP system.

2. Using USB drives for system maintenance:
   NIST 800-53 and NIST 800-171 both require that IT staff check any media containing diagnostic and test programs for malicious code before the media are used in the information system. USB drives should therefore be inserted into a non-TCP machine first and have a virus scan performed on that file system. Once it has been verified that the device is clean, it may be used for TCP system maintenance.

3. Change control:
   The ETS change control process, in its current state of maturity, must be used when making changes to TCP systems. Please copy

   eng-ets-security@osu.edu

   on the change control request form.

These guidelines are provided to highlight controls required by the language in the project contract to help ensure that faculty, staff and students establish workflows that meet compliance guidelines stipulated in the project contract.